



FIM - Windows & Linux

File Integrity Monitoring

Sameer Hassan

Name: Sameer Hassan

SOC ANALYST

Lab # 02

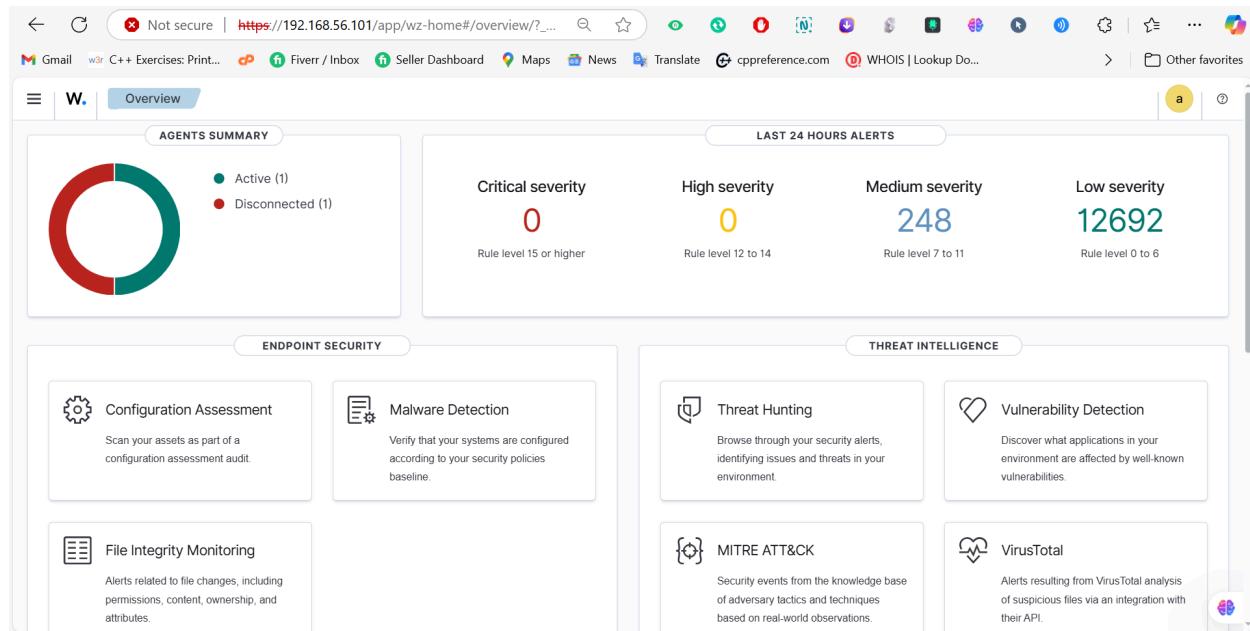
What's FIM?

File Integrity Monitoring (FIM) is a security process that checks and alerts you when your system files are altered, added, or deleted. It helps detect unauthorized changes and ensures the integrity and security of your data.

FIM

- File Integrity Monitoring (FIM) is a security process.
- It checks and alerts you when files are altered, added, or deleted on your system.
- FIM helps detect unauthorized changes.
- It ensures the integrity and security of your data.

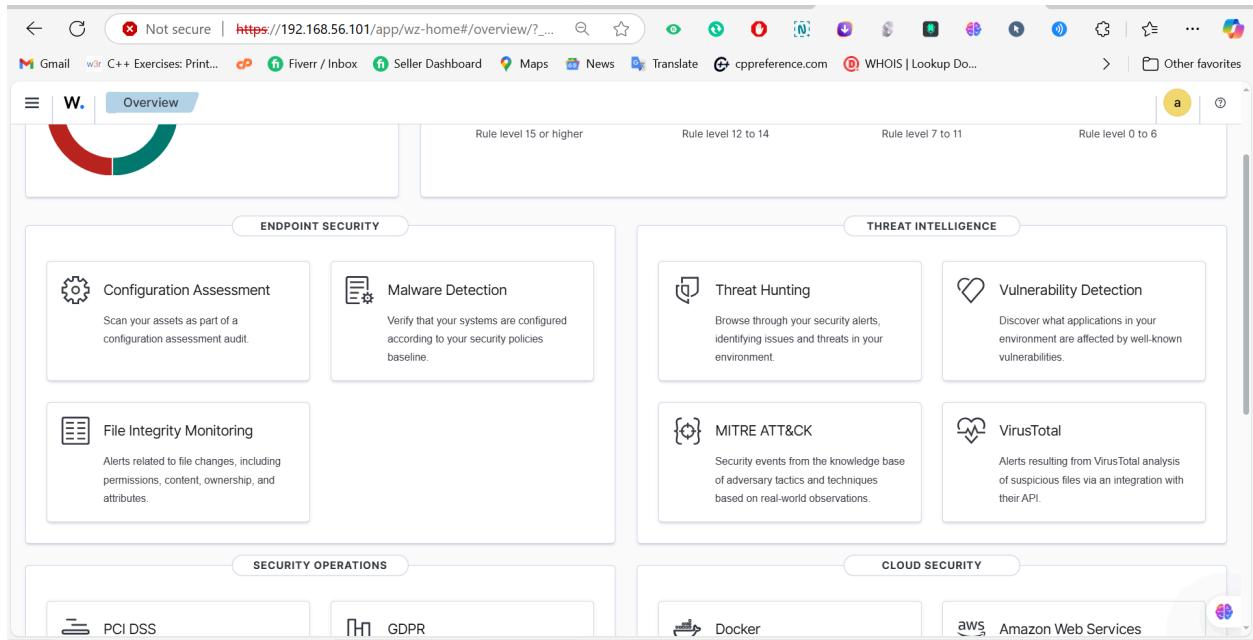
Open Your Wazuh dashboard



I have two Agents integrated with Wazuh 1 is active and 1 is deactivated/Offline.

CONFIGURING FIM

Under Endpoint Security we have a Option named File Integrity Monitoring click on it

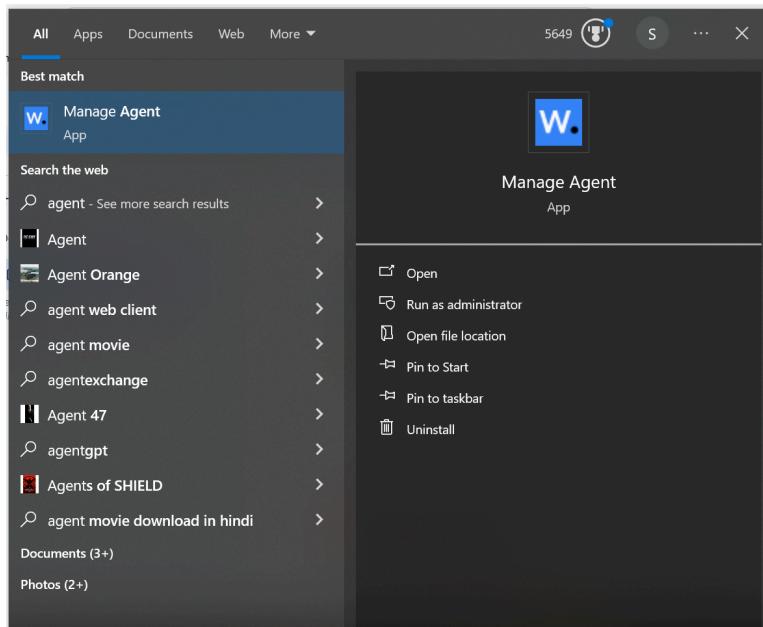


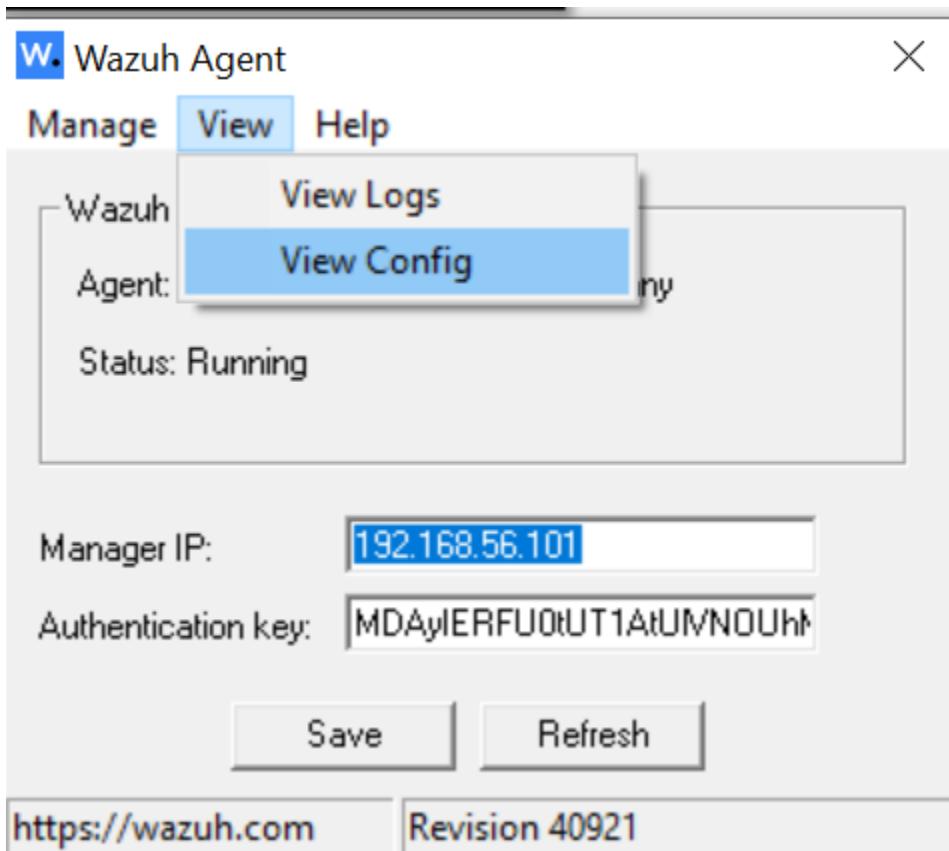
The screenshot shows a web browser window with the following details:

- URL:** Not secure | <https://192.168.56.101/app/file-integrity-monitoring>
- Search Bar:** manager.name: wazuh-server rule.groups: syscheck
- Message:** No results match your search criteria
- Buttons:** DQL, Last 24 hours, Show dates, Refresh

No data is showing.

To configure FIM open Agnet on your Windows OS as administrator.





Click on view then select view Config

It will directly open **OSSEC.CONF** file or you can simply open this file by visiting the OSSEC folder.

Scroll Down and you will found File Integrity Monitoring and Under this, you will find <syschk>
Under this you will see so many Directories tags

```
<directories recursion_level="0"
```

```
restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>
```

Simply add the Folder or drive path you want to monitor.

To add you just replace C:\Users\choice com
<directories realtime="yes" check_all="yes"
report_changes="yes">C:\Users\choice
com</directories>

I added my Choice Com folder to monitor you can add any folder you want!!



```
ossec - Notepad
File Edit Format View Help
<directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
<directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>

<!-- 32-bit programs. -->
<directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg
<directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\drivers\etc</directories>
<directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
<directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

<directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>

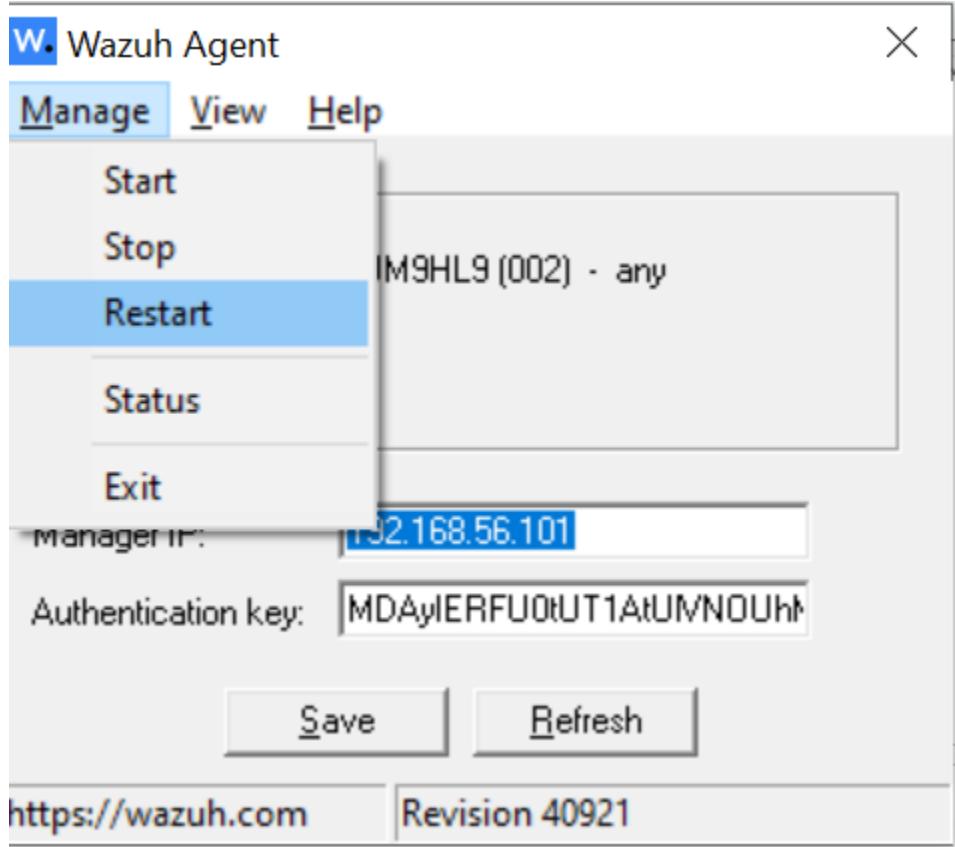
<directories realtime="yes" check_all="yes" report_changes="yes">C:\Users\choice com</directories>
<ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

<ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evt$</ignore>

<!-- Windows registry entries to monitor. -->
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\batfile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\cmdfile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\comfile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\exefile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\pifile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\AllFilesystemObjects</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\Directory</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\Folder</windows_registry>
<windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Classes\Protocols</windows_registry>
<windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Policies</windows_registry>
<windows_registry arch="both">HKEY_LOCAL_MACHINE\Security</windows_registry>
<windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer</windows_registry>

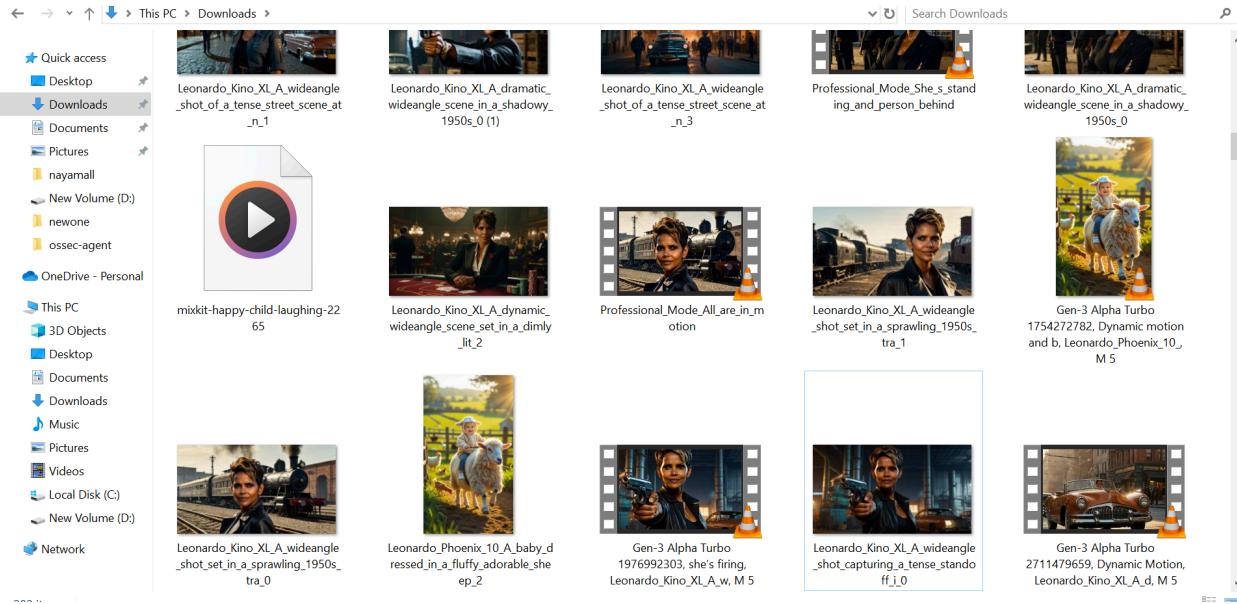
<windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control</windows_registry>
```

After writing this command save the file and Restart the agent!

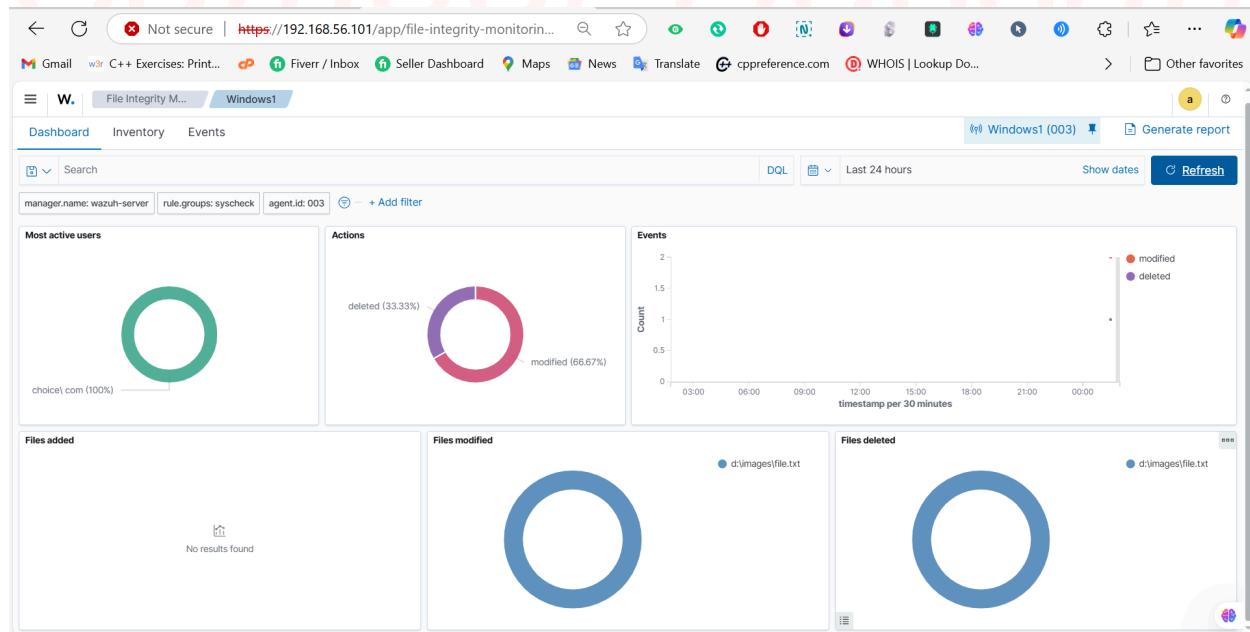


Testing the Configuration

You can delete, Edit or remove any file from the folder you added and you will see the log in Wazuh



Perform any action on file you will see the result in Wazuh.
I deleted 2 files, let's check the Logs.

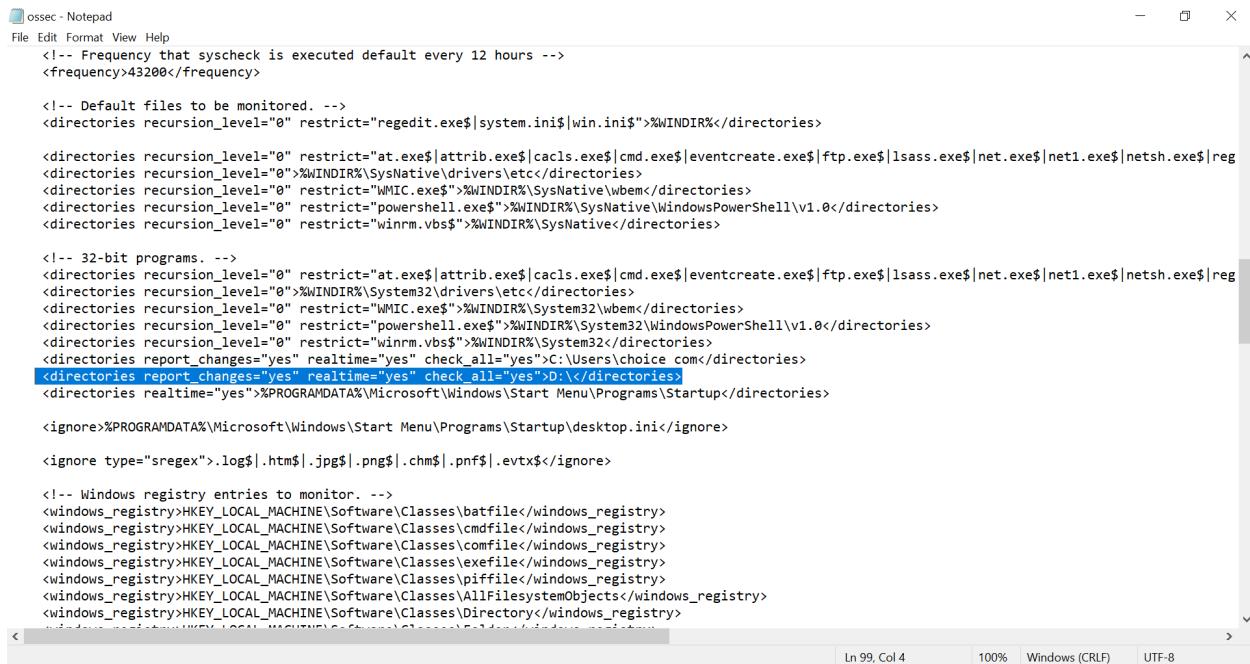


Successfully Configured!

Verification

Add the path of any folder you want to monitor.

I added my D drive path.



The screenshot shows a Notepad window with configuration XML code. The code defines monitoring rules for various system paths, including registry keys and file types. A specific rule for the D drive is highlighted:

```
<!-- 32-bit programs. -->
<directories recursion_level="0" restrict="at.exe$|attrib.exe$|acl$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg
<directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
<directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

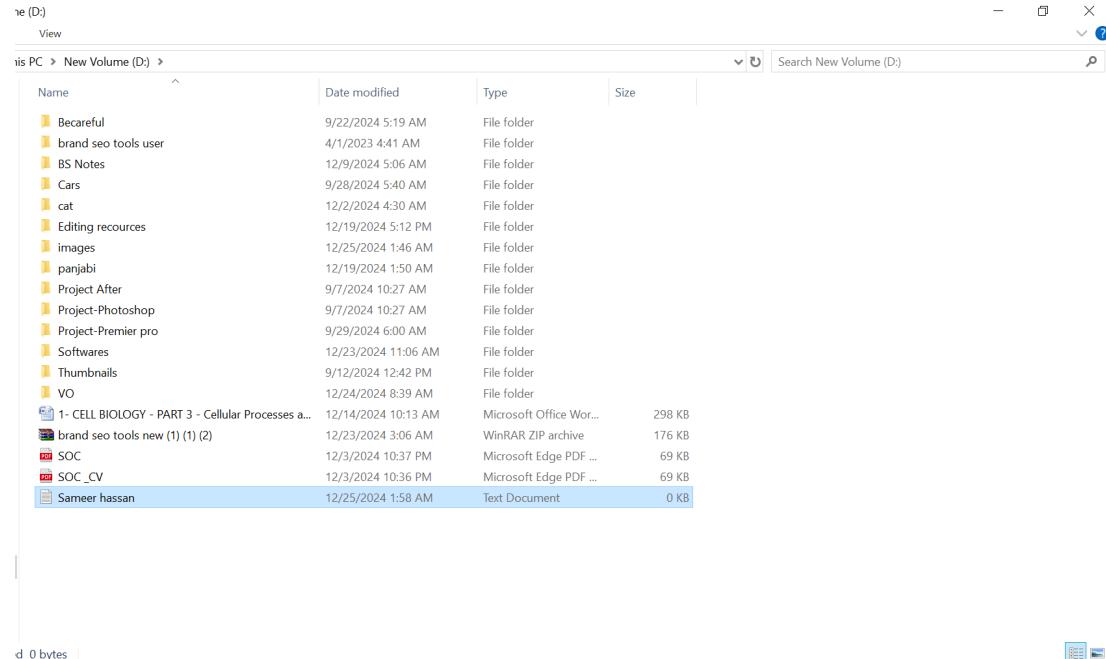
<!-- 32-bit programs. -->
<directories recursion_level="0" restrict="at.exe$|attrib.exe$|acl$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg
<directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
<directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>
<directories report_changes="yes" realtime="yes" check_all="yes">c:\Users\choice\com</directories>
<directories report_changes="yes" realtime="yes" check_all="yes">d:\</directories>
<directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>

<ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>
<ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>

<!-- Windows registry entries to monitor. -->
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\batfile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\cmdfile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\comfile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\exefile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\pifile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\AllFilesystemObjects</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\Directory</windows_registry>
```

After adding the path restart the agent!

Now let's create a new file and add some text to it.

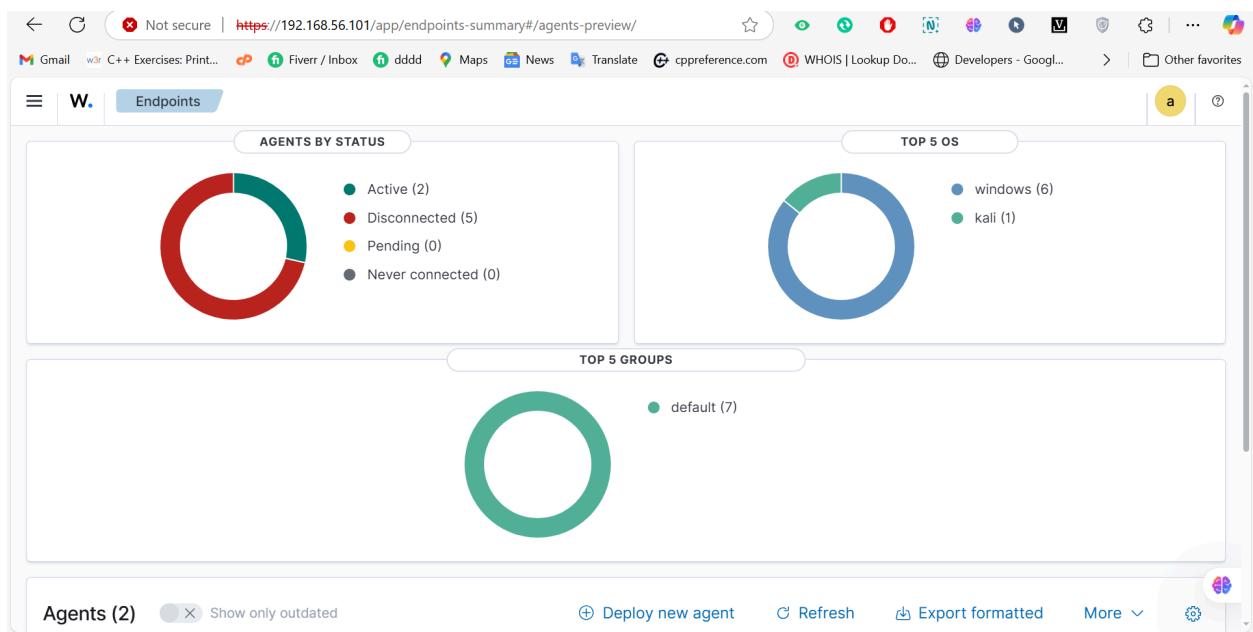


I created a new file named Sameer Hassan let check Wazuh to view the file D drive log.

A screenshot of the Wazuh User Interface (UI) showing event logs for a file modification. The interface includes a search bar, filter options, and a timeline chart. Below the chart is a table of event details, showing three hits for file modifications on 'Windows1'. The table columns include timestamp, agent.name, syscheck.path, syscheck.event, rule.description, rule.level, and rule.id. The events listed are: 1. Dec 25, 2024 @ 01:46:26.491, Windows1, d:\images\file.txt, deleted, File deleted., 7, 553. 2. Dec 25, 2024 @ 01:45:39.051, Windows1, d:\images\file.txt, modified, Integrity checksum changed., 7, 550. 3. Dec 25, 2024 @ 01:44:04.722, Windows1, d:\images\file.txt, modified, Integrity checksum changed., 7, 550.

Windows FIM is Configured!

Now let's configure the Ubuntu Environment FIM.



Two agents are active Windows and another is Ubuntu kali-linux.

The terminal window shows the following directory structure and files:

```
(root@kali)-[~/var/ossec/etc]
# ls
client.keys  internal_options.conf  local_internal_options.conf  localtime  ossec.conf  shared  wpk_root.pem
# ls -l
total 0
```

Visit directory /var/ossec/etc and there you will found OSSEC.conf file.

Open file uisng nano ossec.conf or gedit ossec.conf



```
GNU nano 8.2
[--]
Wazuh - Agent - Default configuration for kali 2024.3
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#forum/wazuh
->

ossec_config>
<client>
  <server>
    <address>192.168.56.101</address>
    <port>554</port>
    <protocol>tcp</protocol>
  </server>
  <config-profile>kali, kali2024, kali2024.3</config-profile>
  <notify_time>10</notify_time>
  <auto_reconnect>yes</auto_reconnect>
  <auto_restart>yes</auto_restart>
  <crypto_method>aes</crypto_method>
  <enrollment>
    <enabled>yes</enabled>
    <agent_name>hasanakali</agent_name>
    <authorization_pass_path>etc/authd.pass</authorization_pass_path>
  </enrollment>
</client>

<client_buffer>
  <!-- Agent buffer options -->
  <disabled>no</disabled>
  <queue_size>8000</queue_size>
  <events_per_second>500</events_per_second>
</client_buffer>

<!-- Policy monitoring -->
<syscheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_devs>yes</check_devs>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>

```

File menu: Help, Exit, Write Out, Read File, Where Is, Replace, Cut, Paste, Execute, Justify, Location, Go To Line, Undo, Redo, Set Mark, To Bracket, Where Was, Previous, Next, Back, Forward, Prev Word, Next Word, Home, End.

After opening the OSSEC.CONF file visit File Integrity Monitoring section as we did in the Windows FIM section.



```
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>
  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>
  <scan_on_start>yes</scan_on_start>
  <!-- Directories to check (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin/directories>
  <directories>/bin,/sbin,/boot/directories>
  <!-- File/directories to ignore -->
  <ignore>/etc/mtab/</ignore>
  <ignore>/etc/hosts.deny/</ignore>
  <ignore>/etc/mail/statistics/</ignore>
  <ignore>/etc/random-seed/</ignore>
  <ignore>/etc/random-seed/</ignore>
  <ignore>/etc/adjtime/</ignore>
  <ignore>/etc/hostname/</ignore>
  <ignore>/etc/utmpx/</ignore>
  <ignore>/etc/utmpx/</ignore>
  <ignore>/etc/cups/certs/</ignore>
  <ignore>/etc/cups/dumpfiles/</ignore>
  <ignore>/etc/svc/volatile/</ignore>
  <!-- File types to ignore -->
  <ignore type="regex">.log$|.swp$</ignore>
  <!-- Check the file, but never compute the diff -->
  <nodiff>/etc/ssl/private.key</nodiff>
  <skip_nfsyes>/skip_nfs</skip_nfs>
  <skip_devyes>/skip_dev</skip_dev>
  <skip_procyes>/skip_proc</skip_proc>
  <skip_sysyes>/skip_sys</skip_sys>
  <!-- Nice value for Syscheck process -->
  <process_priority>10</process_priority>

```

File menu: Help, Exit, Write Out, Read File, Where Is, Replace, Cut, Paste, Execute, Justify, Location, Go To Line, Undo, Redo, Set Mark, To Bracket, Where Was, Previous, Next, Back, Forward, Prev Word, Next Word, Home, End.



Copy directory path you want to add in FIM
I copied my download path.

```
GNU nano 8.2                               ossec.conf *

<!-- File integrity monitoring -->
<syscheck>
<disabled>no</disabled>

<!-- Frequency that syscheck is executed default every 12 hours -->
<frequency>43200</frequency>

<scan_on_start>yes</scan_on_start>

<!-- Directories to check (perform all possible verifications) -->
<directories>/etc,/usr/bin,/usr/sbin/directories>
<directories>/bin,/sbin,/boot</directories>
<directories>/home/panda/Downloads</directories>
<!-- File/directories to ignore -->
<ignore>/tmp/</ignore>
<ignore>/etc/hosts.deny</ignore>
<ignore>/etc/mail/statistics</ignore>
<ignore>/etc/random-seed</ignore>
<ignore>/etc/random-seed</ignore>
<ignore>/etc/adjtime</ignore>
<ignore>/etc/atomics</ignore>
<ignore>/etc/utmpx</ignore>
<ignore>/etc/utmpx</ignore>
<ignore>/etc/cups/certs</ignore>
<ignore>/etc/dumpdates</ignore>
<ignore>/etc/svc/volatile</ignore>

<!-- File types to ignore -->
<ignore type="sregex">>.log$|.swp$</ignore>

<!-- Check the file, but never compute the diff -->
<nodiff>/etc/ssl/private.keys</nodiff>

<skip_nfsyes></skip_nfs>
<skip_devyes></skip_dev>
<skip_procyes></skip_proc>
<skip_sysyes></skip_sys>

<!-- Nice value for syscheck process -->
<process_priority>10</process_priority>
```

I added my Download directory path
You can add this using
<directories check_all="yes">/home/panda/Downloads</directories>

After adding the path save the file and restart the agent. Using command systemctl restart wazuh-agent

```
(panda㉿kali)-[~]
$ sudo systemctl restart wazuh-agent
```

A screenshot of a terminal window on a Kali Linux desktop. The window title is '(panda㉿kali)-[~]'. Inside, the command '\$ sudo systemctl restart wazuh-agent' is typed in blue. The background of the desktop shows a large, faint watermark of a person's face with the text 'KALI PURPLE' overlaid.

Sameer Hassan

Summary

Wazuh's File Integrity Monitoring provides comprehensive monitoring capabilities, ensuring the security and integrity of your files. It tracks changes in real-time, detects unauthorized modifications, and offers detailed reports for enhanced protection against potential threats and data breaches.

Sameer Hassan